(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
28 juillet 2005 (28.07.2005)

(10) Numéro de publication internationale
WO 2005/069122 A3

(51) Classification internationale des brevets :
*G06F 7/72* (2006.01) *G06F 21/00* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2004/053472

(22) Date de dépôt international :
14 décembre 2004 (14.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0314959 19 décembre 2003 (19.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne Parc, d'activités de Gémenos, F-13420 Gemenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **CHEVALLIER-MAMES, Benoit** [FR/FR]; La Sardanne Résidence Les Brayes, F-13260 Cassis (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) Date de publication du rapport de recherche internationale: 1 juin 2006

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

(54) **Title:** METHOD FOR MODULAR EXPONENTIATION, PROTECTED AGAINST DPA-TYPE ATTACKS

(54) **Titre :** PROCEDE CRYPTOGRAPHIQUE D'EXPONENTIATION MODULAIRE PROTEGE CONTRE LES ATTAQUES DE TYPE DPA

(57) **Abstract:** The invention relates to the protection of cryptographic methods against DPA-type covert channel attacks and, in particular, to a cryptographic method during which an x^d-type modular exponentiation is performed, wherein d is a whole number exponent of m+1 bits, consisting in: scanning the d bits from left to right in a loop subscripted by i varying between m and 0; and, with each revolution of rank i, calculating and saving an updated partial result equal to x^b(i) in an accumulator (R0), b(i) being the most significant m-i+1 bits of exponent d ( b (i) = $d_{m->i}$). According to the invention, at the end of a revolution of randomly-selected rank i(j) (i = i(0)), a randomisation step E1 is performed, consisting in subtracting a random number z (z= b(i(j)), z = b (i(j)) $.2^{t}$, z = u) from part of the d bits that have not yet been used ($d_{i-1->0}$) in the method. Subsequently, once the d bits modified by randomisation step E1 have been used, a consolidation step E2 is performed, consisting in saving (R0 <- R1xR0), in the accumulator (R0), the result of the multiplication of the contents of the accumulator (x^b(i)) by a number that is a function of x^z stored in a registry (R1).

(57) **Abrégé :** Dans le domaine de la protection des procédés cryptographiques contre les attaques à canaux cachés de type DPA, l'invention concerne un procédé cryptographique au cours duquel on réalise une exponentiation modulaire de type x^d, avec d un exposant entier de m+1 bits, en balayant les bits de d de gauche à droite dans une boucle indicée par i variant de m à 0 et en calculant et en mémorisant dans un accumulateur (RO), à chaque tour de rang i, un résultat partiel actualisé égal à x^b(i), b(i) étant les m-i+1 bits de poids les plus forts de l'exposant d ( b (i) = $d_{m->i}$) .Selon l'invention, à la fin d'un tour de rang i(j) (i = i(0)) choisi aléatoirement, on réalise une étape E1 de randomisation au cours de laquelle E1: on soustrait un nombre z (z= b(i(j)), z = b (i(j)) $.2^{\tau}$, z = u) aléatoire à une partie des bits de d non encore utilisés ( $d_{i-1->0}$) dans le procédé puis, après avoir utilisé les bits de d modifiés par l'étape de randomisation E1, on réalise une étape de consolidation E2 au cours de laquelle: E2 : on mémorise (R0 <- R1xR0) dans l'accumulateur (RO) le résultat de la multiplication du contenu de l'accumulateur (x^b(i)) par un nombre fonction de x^z mémorisé dans un registre (R1).

WO 2005/069122 A3

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053472

**A. CLASSIFICATION OF SUBJECT MATTER**
G06F7/72 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| T | CHEVALLIER-MAMES B: "Self-randomized exponentiation algorithms" TOPICS IN CRYPTOLOGY - CT-RSA 2004. PROCEEDINGS. SPRINGER-VERLAG, LECTURE NOTES IN COMPUTER SCIENCE, vol. 2964, 27 February 2004 (2004-02-27), pages 236-249, XP002297836 BERLIN, GERMANY ISBN: 3-540-20996-4 the whole document | 1-21 |
| A | FR 2 829 646 A (GEMPLUS CARD INT) 14 March 2003 (2003-03-14) abstract | 1-21 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 27 March 2006 | 05/04/2006 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Carnerero Álvaro, F |

Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/053472

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 01/31436 A (BULL CP8 ; GOUBIN LOUIS (FR)) 3 May 2001 (2001-05-03)<br>page 6 - page 7<br>page 10 | 1-21 |
| A | WALTER C D: "MIST: AN EFFICIENT, RANDOMIZED EXPONENTIATION ALGORITHM FOR RESISTING POWER ANALYSIS"<br>LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US,<br>vol. 2271, 18 February 2002 (2002-02-18), pages 53-66, XP008004946<br>ISSN: 0302-9743<br>cited in the application<br>page 53 - page 57 | 1-21 |
| A | JOYE M: "Recovering lost efficiency of exponentiation algorithms on smart cards"<br>ELECTRONICS LETTERS, IEE STEVENAGE, GB,<br>vol. 38, no. 19,<br>12 September 2002 (2002-09-12), pages 1095-1097, XP006019065<br>ISSN: 0013-5194<br>the whole document | 1-21 |
| A | ITOH K ET AL: "DPA COUNTERMEASURES BY IMPROVING THE WINDOW METHOD"<br>CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX,<br>13 August 2002 (2002-08-13), pages 303-317, XP001160529<br>cited in the application<br>page 303 - page 310 | 1-21 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/053472

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| FR 2829646 A | 14-03-2003 | WO 03025739 A1 | 27-03-2003 |
| WO 0131436 A | 03-05-2001 | FR 2800478 A1 | 04-05-2001 |
| | | JP 2003513491 T | 08-04-2003 |
| | | US 6973190 B1 | 06-12-2005 |

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/053472

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**
G06F7/72 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| T | CHEVALLIER-MAMES B: "Self-randomized exponentiation algorithms" TOPICS IN CRYPTOLOGY - CT-RSA 2004. PROCEEDINGS. SPRINGER-VERLAG, LECTURE NOTES IN COMPUTER SCIENCE, vol. 2964, 27 février 2004 (2004-02-27), pages 236-249, XP002297836 BERLIN, GERMANY ISBN: 3-540-20996-4 le document en entier | 1-21 |
| A | FR 2 829 646 A (GEMPLUS CARD INT) 14 mars 2003 (2003-03-14) abrégé | 1-21 |

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 27 mars 2006 | 05/04/2006 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Carnerero Álvaro, F |

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/053472

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| A | WO 01/31436 A (BULL CP8 ; GOUBIN LOUIS (FR)) 3 mai 2001 (2001-05-03)<br>page 6 - page 7<br>page 10 | 1-21 |
| A | WALTER C D: "MIST: AN EFFICIENT, RANDOMIZED EXPONENTIATION ALGORITHM FOR RESISTING POWER ANALYSIS"<br>LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US,<br>vol. 2271, 18 février 2002 (2002-02-18), pages 53-66, XP008004946<br>ISSN: 0302-9743<br>cité dans la demande<br>page 53 - page 57 | 1-21 |
| A | JOYE M: "Recovering lost efficiency of exponentiation algorithms on smart cards"<br>ELECTRONICS LETTERS, IEE STEVENAGE, GB,<br>vol. 38, no. 19,<br>12 septembre 2002 (2002-09-12), pages 1095-1097, XP006019065<br>ISSN: 0013-5194<br>le document en entier | 1-21 |
| A | ITOH K ET AL: "DPA COUNTERMEASURES BY IMPROVING THE WINDOW METHOD"<br>CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX,<br>13 août 2002 (2002-08-13), pages 303-317, XP001160529<br>cité dans la demande<br>page 303 - page 310 | 1-21 |

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/EP2004/053472

| Document brevet cité au rapport de recherche | | Date de publication | Membre(s) de la famille de brevet(s) | | Date de publication |
|---|---|---|---|---|---|
| FR 2829646 | A | 14-03-2003 | WO | 03025739 A1 | 27-03-2003 |
| WO 0131436 | A | 03-05-2001 | FR | 2800478 A1 | 04-05-2001 |
| | | | JP | 2003513491 T | 08-04-2003 |
| | | | US | 6973190 B1 | 06-12-2005 |